

Multiparty quantum key agreement protocol secure against collusion attacks

Zhiwei Sun · Xiaoqiang Sun · Ping Wang

Received: date / Accepted: date

Abstract The fairness of a secure multi-party quantum key agreement (MQKA) protocol requires that all involved parties are entirely peer entities and can equally influence the outcome of the protocol to establish a shared key wherein no one can decide the shared key alone. However, it is found that parts of the existing MQKA protocols are sensitive to collusion attacks, i.e., some of the dishonest participants can collaborate to predetermine the final key without being detected. In this paper, a multi-party QKA protocol resisting collusion attacks is proposed. Different from previous QKA protocol resisting $N-1$ conspirators or resisting 1 conspirators, we investigate the general circle-type MQKA protocol which can be secure against t dishonest participants' cooperation. Here, $t < N$. We hope the results of the presented paper will be helpful for further research on fair MQKA protocols.

Keywords Quantum key agreement · collusive attacks · fairness

1 Introduction

Key distribution (KD) allows two authorized participants to establish a shared secret key over a public channel. The shared key can be used for secure communication or authentication protocols. Key agreement (KA) is another important way to establish keys. Compared with the key distribution, in which one party distributes a secret key to the other, all involved parties in a key agreement protocol can equally influence the outcome of the protocol, and no one or a subset of the group can decide the shared key alone. One main difference between key agreement and key distribution is that, key agreement protocols not only need

Zhiwei Sun
Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen, 518060,
P.R.China

Zhiwei Sun · Xiaoqiang Sun · Ping Wang
College of Information Engineering, Shenzhen University, Shenzhen, Guangdong 518060,
P.R.China
E-mail: sunzhiwei1986@gmail.com, wangping@szu.edu.cn

to resist adversaries from the outside world, but also are required to prevent the participant attacks.

The security of the classical key agreement protocols are mainly based on the Diffie-Hellman problem or discrete logarithm problem. With the development of quantum computers and the polynomial-time quantum algorithms for prime factorization and discrete logarithm [1], the security of classical key agreement protocols have become increasingly vulnerable.

Quantum cryptography, which is based on the quantum mechanical, provides another way for secure key distribution. Since it can provide unconditional security. It has been developed quickly and become a hot topic in cryptography, such as quantum secret sharing[2,3], quantum secure direct communication[4,5], quantum private comparison[6,7,8,9,10] and quantum oblivious transfer [11]. Quantum key agreement (QKA) is a new branch of quantum cryptography. Since it was first proposed by Zhou et al. in 2004 [12], lots of QKA protocols have been proposed. In the previously works, only two participants were involved in the QKA protocols [13, 14, 15, 16, 17, 18]. Recently, an enhanced interest on multi-party QKA protocols has been observed [19, 20, 21, 22, 23, 24, 25, 26, 27, 28].

Fairness is an important standard needed to be considered in a secure quantum key agreement protocol. However, it found that most of the quantum key agreement protocols cannot resist collusive attacks [29], i.e., parts of the participants of the group can predetermine the shared key before the end of the protocol. Thus, how to construct a fair and secure key agreement protocol has obtained much attentions.

In this paper, we propose a multiparty quantum key agreement protocol which can resist general collusion attacks. The proposed protocol is based on the idea of our previous multi-party QKA protocol [27]. And the main contribution of the paper is that we present a general way to construct a secure multi-party QKA which can resist t coconspirators. We hope the results of the presented paper will be helpful for further research on fair MQKA protocols.

The rest of this paper is organized as follows. Sect.2 first introduces the formalization of the circle-type multi-party QKA (CT-MQKA) protocols, and the collusion attacks on the CT-MQKA protocols[29]. Then, we present the MQKA protocol against collusion attacks. Precisely speaking, the presented protocol, which is the generalization of the MQKA protocol in Ref. [27], can resist t coconspirators. Here, $t < N$, where N is the number of the participants in the MQKA protocol. The security and efficiency analyses are given in Sect.3. Sect.4 gives a short conclusion.

2 Multi-party quantum key agreement protocol

We first introduce the formalization of the circle-type multiparty quantum key agreement (CT-MQKA) protocols, and the collusion attacks to the CT-MQKA proposed by Liu [29]. Then, we show that the CT-MQKA protocols can be used as sub-protocol to construct secure multiparty QKA against collusion attacks. Usually, suppose there are N participants P_0, \dots, P_{N-1} , and they have secret bit strings keys K_0, \dots, K_{N-1} , respectively. We denote " \boxplus " as addition modular N , and " \boxminus " as subtraction modular N , just like the Ref. [29] does.

2.1 Brief review of the CT-MQKA protocol

At the beginning of the protocol, P_i prepares a sequence of entangled states and divides each entangled states into two parts, one of which will be kept, "the home qubit sequence", and the other will be sent out, "the travel qubit sequence". And, we denote the home qubit sequence as R_i , and travel qubit sequence as S_i , respectively, where $i = 0, 1, \dots, N-1$.

Then all the S_i s are transmitted in the same direction in the circle. When all the participants $P_{i \oplus 1}$ have received S_i , they do the detection and encode their secret keys in the received sequences. Afterwards, they continue to send the above sequence to the next participants. One by one, all the participants will continue the above process. When each travel qubit sequences is sent back to the participant who generated it, i.e., the travel qubit sequence finishes a complete circle, P_i can measure R_i and S_i to get the bitwise exclusive OR results of all the other participant's secret keys. Finally, they can calculate the final key $K_{final} = \bigotimes_{i=0}^{N-1} K_i$.

For the convenience of description, we briefly describe the CT-MQKA protocols of Ref.[21], which is secure against single participant's attack. In Ref.[21], the whole process of the CT-MQKA is divided into N periods.

In the first period, each P_i prepares R_i and S_i ¹, and sends S_i to $P_{i \oplus 1}$. When each $P_{i \oplus (k-1)}$ receives S_i , the k -th period starts. In the k -th period, each $P_{i \oplus (k-1)}$ performs the detection processes with $P_{i \oplus (k-2)}$ to detect the possible attacks on S_i . Then, each $P_{i \oplus (k-1)}$ encodes his/her secret key $K_{i \oplus (k-1)}$ on S_i , and inserts some decoy states in it and sends it to $P_{i \oplus k}$. When the k -th period ends, the $k+1$ period starts. Here, $k = 2, 3, \dots, N-1$.

In the N -th period (a complete circle is finished), each P_i performs the attacks detection with $P_{i \oplus 1}$ as before. After that, the bitwise exclusive OR result of the others' secret keys can be obtained by measuring R_i and S_i . P_i performs the bitwise exclusive OR operation between the above result and K_i to get the final key K_{final} .

2.2 Liu's collusive attacks against CT-MQKA protocol

Liu's collusive attacks can be divided into two stages: the key stealing stage and the key flipping stage [29]. In the key stealing stage, the collusive participants try to get the bitwise exclusive OR result of the others' secret key in some novel way. Then, they try to flip the encoded secret keys according to the above result to control the final key in the key flipping stage.

And, Ref.[29] shows that any two participants P_n and P_m ($n > m$) are enough to totally control the final key, as long as their position in the circle satisfy the following conditions:

$$n - m = \frac{N}{2} \quad \text{for an even } N; \quad (1)$$

$$n - m = \frac{N-1}{2} \text{ or } \frac{N+1}{2} \quad \text{for an odd } N. \quad (2)$$

¹ For the single state, it can be considered as the entangled states where parts of them R_i have already been measured.

When the above conditions are satisfied, P_n and P_m perform the following collusion attacks:

1. **The key stealing stage:**

- In the first period, P_n and P_m share all the information about R_n, S_n, K_n and R_m, S_m, K_m and the value of the expected key $K_{expected}$.
- In the $(n - m)$ -th period which started by P_m , P_n has received the travel sequence S_m . Combined with the shared information about R_m, S_m , P_n can obtain the bitwise exclusive OR result of the secret key $K_{m+1}, K_{m+2}, \dots, K_{n-1}$ by measuring R_m and S_m . Similarly, P_m can get the bitwise exclusive OR result of the secret key $K_{n+1}, K_{n+2}, \dots, K_{m-1}$ by measuring R_n and S_n in the $(N - n + m)$ -th period which started by P_n .
- P_n (P_m) sends the above bitwise exclusive OR result to P_m (P_n) immediately he/she gets it.

2. **The key flipping stage:** In the $\frac{N}{2}$ period (for the convenience of description of the collusion attacks, suppose N is an even number), each of P_n and P_m gets the bitwise exclusive OR result of half of the others' secret key. After exchanging with each other, they get the legal final key K_{final} ahead of others. Then P_n and P_m can predetermine the final key by encode $K'_n = K_n + K_{expected} + K_{final}$ instead of K_n , and $K'_m = K_m + K_{expected} + K_{final}$ instead of K_m respectively in the rest periods. It can be verified that, in the last period, for any participant P_i , he/she will get the final key is $K_{final} = K_{expected}$.

2.3 Multi-party QKA protocol against t coconspirators

Recently, Sun et. al. proposed a novel multi-party quantum key agreement protocol by using entangled states [27], which is secure against 2 collusion attackers. In their protocol, each participant sends out two sequences, instead of one sequence in CT-MQKA. Each of the two sequences "runs" half circle. Two collusive participants cannot succeed any more by using Liu's collusion attacks. Because each of them can only get the bitwise exclusive OR result of half of the other's personal keys after the last period, which leaves no time for them to flip the others' sequences. However, when three participants collaborate with each other, they can be succeed. Thus, Sun et. al.'s protocol can be only secure against 2 coconspirators. Even though more than two participants can succeed in attacking Sun et. al.'s MQKA protocol, it provides a new perspective for in-depth analysis of multi-party QKA protocols secure against collusion attacks.

Suppose there are N participants involved in the multi-party QKA protocol. And, we hope it can resist t dishonest participants' cooperation, where $t \leq \frac{N}{2}$. And the N participants are arranged uniformly in the circle. The proposed multi-party QKA protocol against t coconspirators is described as follows.

1. In the first period, each P_i prepares t sequences of entangled states, and divides each entangled states into two parts $(R_i^0, S_i^0), \dots, (R_i^{t-1}, S_i^{t-1})$ ², respectively, and sends S_i^0 to $P_{i \oplus 1}$, S_i^1 to $P_{i \oplus \lfloor \frac{N}{t} \rfloor \oplus 1}$, \dots , S_i^{t-1} to $P_{i \oplus \lfloor \frac{(t-1)N}{t} \rfloor \oplus 1}$. Here, $\lfloor x \rfloor$ represents the maximum integer which is not more than x . For the convenience

² For the single state, it can be considered as the entangled states where parts of them have already been measured.

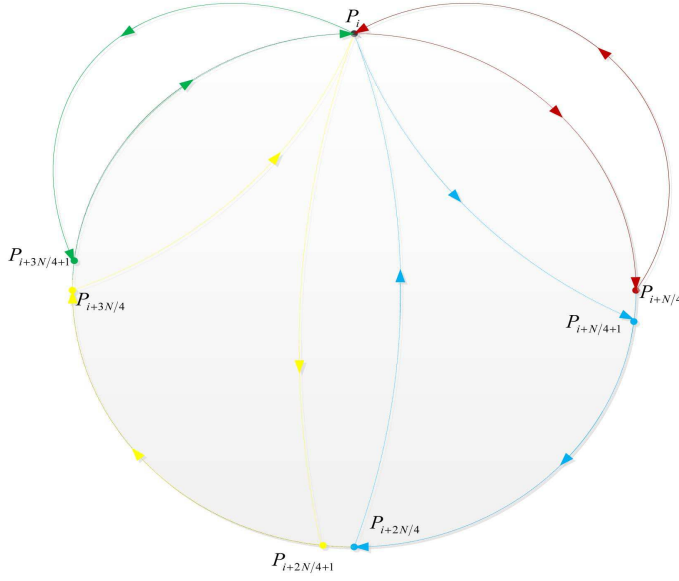


Fig. 1 We give an example for $t = 4$, i.e., the MQKA can resist 4 collusive attackers. The circle is divided into 4 parts, the red part, the blue part, the yellow part and the green part. Each part is a complete sub-circle when S_i is returned back to P_i .

of description, we simply write $\frac{N}{t}$ instead of $\lfloor \frac{N}{t} \rfloor$. Note that P_i divides the circle into t parts, each part has $\frac{N}{t}$ participants.

2. **Detection phase** When each $P_{i \oplus (k-1)}$ receives S_i^0 , $P_{i \oplus \frac{N}{t} \oplus (k-1)}$ receives S_i^1 , \dots , $P_{i \oplus \frac{(t-1)N}{t} \oplus (k-1)}$ receives S_i^{t-1} , respectively, the k -th period starts. Here, $k = 2$.

In the k -th period, each $P_{i \oplus (k-1)}$ first performs the detection processes with $P_{i \oplus (k-2)}$ to detect the possible attacks on S_i^0 , $P_{i \oplus \frac{N}{t} \oplus (k-1)}$ first performs the detection processes with $P_{i \oplus \frac{N}{t} \oplus (k-2)}$ to detect the possible attacks on S_i^1 , \dots , $P_{i \oplus \frac{(t-1)N}{t} \oplus (k-1)}$ first performs the detection processes with $P_{i \oplus \frac{(t-1)N}{t} \oplus (k-2)}$ to detect the possible attacks on S_i^{t-1} , respectively.

Note that, in the second period, $P_{i \oplus 1}$, $P_{i \oplus \frac{N}{t} \oplus 1}$, \dots , $P_{i \oplus \frac{(t-1)N}{t} \oplus 1}$ perform detection process with P_i , instead of their former participant in the circle, to detect the possible attacks.

3. **Encoding Phase** When all the sequences are secure, each $P_{i \oplus (k-1)}$ encodes his/her secret key $K_{i \oplus (k-1)}$ in S_i^0 , and inserts some decoy states in it and sends it to $P_{i \oplus k}$, $P_{i \oplus \frac{N}{t} \oplus (k-1)}$ encodes his/her secret key $K_{i \oplus \frac{N}{t} \oplus (k-1)}$ in S_i^1 , and inserts some decoy states in it and sends it to $P_{i \oplus \frac{N}{t} \oplus k}$, \dots , $P_{i \oplus \frac{(t-1)N}{t} \oplus (k-1)}$ encodes his/her secret key $K_{i \oplus \frac{(t-1)N}{t} \oplus (k-1)}$ in S_i^{t-1} , and inserts some decoy states in it and sends it to $P_{i \oplus \frac{(t-1)N}{t} \oplus k}$, respectively.

4. The parties sequentially execute eavesdropping check and the encoding processes in the same way as participants did in steps 2 and 3. When the k -th period ends, the $k + 1$ period starts. Here, $k = 2, \dots, \frac{N}{t}$.
5. In the $\frac{N}{t} + 1$ -th period (a complete sub-circle is finished, for example Fig.1), each $P_{i \oplus \frac{N}{t}}, P_{i \oplus \frac{2N}{t}}, \dots, P_{i \oplus t \lfloor \frac{N}{t} \rfloor}$ performs the attacks detection with P_i , respectively. After that, the bitwise exclusive OR result of the others' secret keys can be obtained by measuring $(R_i^0, S_i^0), \dots, (R_i^{t-1}, S_i^{t-1})$. P_i performs the bitwise exclusive OR operation between the above result and K_i to get the final key K_{final} .

3 Security and Efficiency analysis

In this section, we will give the security and efficiency analysis of the proposed multi-party QKA protocol.

3.1 Security analysis

We first consider $t > \frac{N}{2}$. When $N > t > \frac{N}{2}$, we have $1 < \frac{N}{t} < 2$, i.e., $\lfloor \frac{N}{t} \rfloor = 1$. In this case, the circle will be divided into N parts, each part has 1 participant. Then, this kind of CT-MQKA protocol becomes the complete-graph-type MQKA (CGT-MQKA) protocol [18, 20, 23], which has been proven fair against both single and collusion attacks.

When $t < \frac{N}{2}$. For the simplest case $t = 1$, the proposed multi-party QKA protocol becomes the standard circle-type multi-party QKA (CT-MQKA) protocol [21, 22, 26], which has been proven that it is secure against single participant attack.

For the general case, the security analysis is similar to the security analysis of the MQKA protocol resisting 2 coconspirators [27]. As we know, Liu's collusive attacks can be divided into two stages: the key stealing stage and the key flipping stage. In the key stealing stage, the collusive participants try to get the bitwise exclusive OR result of the others' secret key. Then, they can flip the encoded secret keys according to the above result to control the final key in the key flipping stage. In order to resist Liu's collusion attacks, the key stealing stage or the key flipping stage must be destroyed. It can be verified that the proposed protocol cannot resist collusion attack at the key stealing stage. In other words, t participants, in the special positions of the circle, can get the final key ahead of others, by using Liu's collusion attacks. However, when the key stealing stage is finished, the whole protocol is also accomplished, i.e., the collusive participants have no time to flip the encoded secret keys. The key flipping stage is destroyed. Thus, the t coconspirators cannot predetermine the final key any more. For the precise security analysis, it can refer to Ref. [20, 27].

3.2 Efficiency analysis

We use the qubit efficiency to measure the efficiency of the proposed MQKA protocol. The qubit efficiency was introduced by Cabello [30] in 2000, which is

given as

$$\eta = \frac{c}{q + b}, \quad (3)$$

where c denotes the length of the transmitted message bits (the length of the final key), q is the number of the used qubits, and b is the number of classical bits exchanged for decoding of the message (classical communication used for checking of eavesdropping is not counted).

In order to generate n bits of shared key, each party has to prepare $t.n$ single photons and $\kappa t.n$ decoy particles in the proposed protocol. There is no classical bits exchanged for decoding of the shared key. Hence, the qubit efficiency of proposed protocol can be computed, $\eta = \frac{n}{(tn + \kappa tn)N} = \frac{1}{(\kappa + 1)tN}$, where κ is the detection rate and N is the number of the participants. It can be verified that when $t = N - 1$, the qubit efficiency is $\frac{1}{(\kappa + 1)N(N - 1)}$, which is identical to the qubit efficiency of Ref. [20]. This also implies that the proposed protocol is a general case of MQKA protocol resisting t coconspirators.

4 Conclusion

In conclusion, we propose a multiparty quantum key agreement protocol which can resist collusion attacks which is presented in the Ref. [29]. The proposed protocol is based on the idea of our multi-party QKA protocol which can resist 2 coconspirators [27]. And the main contribution of the paper is that we present a general way to construct a secure multi-party QKA which can resist t participants collaborating to predetermine the final key, which protects the honest participants' fairness. We hope the results of the presented paper will be helpful for further research on more secure and more fair MQKA protocols.

Acknowledgements This work is funded by the National Natural Science Foundation of China (No. 61402293, 61300204), the Science and Technology Innovation Projects of Shenzhen (No. JCYJ20150324141711665 and No. JCYJ20150324141711694), Natural Science Foundation of SZU (No. 201435), Shenzhen R&D Program (GJHZ20140418191518323), Seed Funding from Scientific and Technical Innovation Council of Shenzhen Government (No. 827-000035), Natural Science Foundation of Guangdong (2015A030313630), Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, and China Postdoctoral Science Foundation (No. 2015M572360).

References

1. Shor P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings of 35th Annual Symposium on the Foundations of Computer Science, pp.124-134 (1994)
2. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A 59, 1829 (1999)
3. Du, R.G., Sun, Z.W., Wang, B.H., Long, D.Y.: Quantum secret sharing of secure direct communication using one-time pad. Int. J. Theor. Phys. 51, 2727-2736 (2012)
4. Sun, Z.W., Du, R.G., Long, D.Y.: Quantum secure direct communication with quantum identification. Int. J. Quantum Inf. 10, 1250008 (2012)
5. Sun, Z.w., Du, R.G., Long, D.Y.: Quantum secure direct communication with two-photon four-qubit cluster state, Int. J. Theor. Phys., 51, 1946-1952 (2012).

6. LIU, W. J., LIU, C., LIU, Z. H., LIU, J. F. and GENG, H. T: Same Initial States Attack in Yang et al.'s Quantum Private Comparison Protocol and the Improvement. *International Journal of Theoretical Physics*. 53(1), pp.271-276 (2014)
7. LIU, W.-J., LIU, C., CHEN, H.-W., LIU, Z.-H., YUAN, M.-X. and LU, J.-S: Improvement on "an efficient protocol for the quantum private comparison of equality with W state". *Int J Quantum Inf*. 12(01), 1450001 (2014)
8. LIU, W. J., LIU, C., CHEN, H. W., LI, Z. Q. and LIU, Z. H: Cryptanalysis and Improvement of Quantum Private Comparison Protocol Based on Bell Entangled States. *Communications in Theoretical Physics* 62(2), pp.210-214 (2014)
9. Sun, Z.w., Long, D.Y.: Quantum private comparison protocol based on cluster states, *Int. J. Theor. Phys.*, 52, 212-218 (2013).
10. Sun, Z.W., Yu, J.P., Wang, P., Xu, L.L., Wu, C.H.: Quantum private comparison with a malicious third party. *Quantum Inf. Process*, 14(6): 2125-2133 (2015).
11. Zhiwei Sun, Jianping Yu, Ping Wang, Lingling Xu: Symmetrically private information retrieval based on blind quantum computing, *Phys. Rev. A* 91, 052303 (2015).
12. Zhou, N., Zeng, G., Xiong, J.: Quantum key agreement protocol. *Electronics Letters* 40(18), 1149 (2004)
13. Tsai, C., Hwang, T.: On quantum key agreement protocol. Technical Report, C-S-I-E, NCKU, Taiwan, R.O.C (2009)
14. Chong, S.K., Tsai, C.W., Hwang, T.: Improvement on Quantum Key Agreement Protocol with Maximally Entangled States. *Int. J. Theor. Phys.* 50(6), 1793-1802 (2011)
15. Chong, S.K., Hwang, T.: Quantum key agreement protocol based on BB84. *Opt. Commun.* 283(6), 1192-1195 (2010)
16. Huang, W., Wen, Q.Y., Liu, B., Gao, F., Sun, Y.: Quantum key agreement with EPR pairs and single particle measurements. *Quantum Inf. Process* 13(3), 649-663 (2014)
17. Shen Dongsu, Ma Wenping, Wang Lili: Two-party quantum key agreement with four-qubit cluster states. *Quantum Inf. Process.*, 13, 2313 (2014).
18. He. Y. F., Ma W. P.: Quantum key agreement protocols with four-qubit cluster states. *Quantum Inf. Process* 14(9), 3483-3498 (2015)
19. Shi, R.H., Zhong, H.: Multi-party quantum key agreement with bell states and bell measurements. *Quantum Inf. Process* 12(2), 921-932 (2013)
20. Liu, B., Gao, F., Huang, W., Wen, Q.y.: Multiparty quantum key agreement with single particles. *Quantum Inf. Process* 12(4), 1797-1805 (2013)
21. Sun Z., Wang B., Li Q., Long D.: Improvements on multiparty quantum key agreement with single particles. *Quantum Inf. Process.*, 12, 3411 (2013).
22. Yin, X.R., Ma, W.P., Liu, W.Y.: Three-party quantum key agreement with two-photon entanglement. *Int. J. Theor. Phys.* 52, 3915-3921 (2013)
23. Yin, X. R., Wen. W. P., Shen D. S., et al.: Three-party quantum key agreement with Bell states, *Acta Physica Sinica* 62(17), 170304 (2013)
24. Chitra, S., Nasir, A., Anirban, P.: Protocols of quantum key agreement solely using Bell states and Bell measurement. *Quantum Inf. Process.* 13, 2391-2405 (2014)
25. Zhu Z. C., Hu A. Q., Fu A. M.: Improving the security of protocols of quantum key agreement solely using Bell measurement, *Quantum Inf. Process.* 14(11), 4245-4254 (2015)
26. Zhiwei Sun, Jianping Yu, Ping Wang, Efficient multiparty quantum key agreement by cluster states. *Quantum Inf. Process.*, 15(1), pp. 373-384 (2016)
27. Sun Z., Zhang C., Wang P., Yu J., Zhang Y. Long D.: Multi-party quantum key agreement by an entanglement six-qubit state, *Int. J. Theor. Phys.*, DOI 10.1007/s10773-015-2831-8, (2015)
28. Huang W., Wen Q. Y., Liu B., et al.: Cryptanalysis of a multi-party quantum key agreement protocol with single particles. *Quantum Inf Process.* 13(7), pp. 1651-1657, 2014.
29. Liu B., Di Xiao, Heng-Yue Jia, Run-Zong Liu: Collusive attacks to circle-type multi-party quantum key agreement protocols. *Quantum Inf Process.* DOI:10.1007/s11128-016-1264-5, 2016
30. Cabello, A.: Quantum key distribution in the Holevo limit. *Phys. Rev. Lett.* 85: 5633-5638 (2000).